Last time: 1) A primitive root mod m is a residue \( r \) s.t. \( \text{ord}_m(r) = \phi(m) \) (largest possible) \( (r, m) = 1 \).

Then \( U(m) = \{ a \mod m \mid (a, m) = 1 \} = \{ r^i \mid 0 \leq i \leq \phi(m) - 1 \} \).

2) Primitive roots exist iff \( m \in \{2, 4, p^k, 2p^k \mid p \text{ odd prime} \} \) (PF today).

3) Discrete log: given \( r^j = b \), give \( r, b \) find \( j \).
   (Has the usual properties of logarithms, since \( r^{i+j} = r^i \cdot r^j \).
   So also \( r^{i+j} = r^i \cdot (r^j)^{i} \) (mod \( \phi(m) \)).

4) Use this to solve equations: if \( r^i = b \) then \( \text{equation } x^n = b(m) \) is equivalent to \( ny = j \) (mod \( \phi(m) \))
   by change of variable \( x = r^y \).

Today: 1) proof of existence of primitive roots mod \( p \)

2) Diffie-Hellman key exchange

3) with power residues mod \( p \).
Thm: Let \( p \) be prime. Then, there exist primitive roots mod \( p \), (actually \( \phi(p-1) \) of them).

Pf: Idea: count how many residue classes mod \( p \) have each order dividing \( p-1 \).

Ingredients: (1) Every non-zero residue mod \( p \) is invertible.

**⇒** (2) A polynomial of degree \( d \) has at most \( d \) roots mod \( p \).

(Sketch: if \( f(x) \) has root \( a \) \( \rightarrow \) then \( x-a \) divides \( f(x) \).

But every root of \( f \) other than \( a \) must be a root of \( g \).)

(3) \( n = \sum_{d \mid n} \phi(d) \)

If of this: let \( n = p-1 \) so the order of each \( a \) mod \( p \) divides \( n \). Goal: for each \( d \mid n \), exactly \( \phi(d) \) classes of order \( d \).

For this, let \( a \) have order \( d \) mod \( p \), where \( d \mid n = p-1 \).

(Fermat's Little Thm: \( \text{ord}_p(a) \mid p-1 \) for all \( a \neq 0 \) (mod \( p \)).

If \( a \) has order \( d \), \( a \) is a root of the polynomial \( x^d - 1 \).

Note: \( b^d \equiv 1 \) (mod \( p \)) if \( \text{ord}_p(b) \mid d \) so \( \{ \text{roots of } x^d - 1 \} = \{ \text{classes of order } d \} \).

⇒ at most \( d \) classes of order dividing \( d \).

On the other hand, the \( d \) distinct classes \( \{ a^{dj} \} \) have order dividing \( d \): \( (a^{dj})^d = a^{dj} \cdot a^{dj} \cdot a^{dj} = (a^d)^j \equiv 1 \) (mod \( p \)).
If \( a \) has order \( d \) mod \( p \), \( \{ a^i \}_{i=0}^{d-1} \) are exactly the classes having order dividing \( d \).

Next step: count classes of order \( d \) exactly, \( d/2 \) or \( d \).

Example: say 2|d. The \( a^2 \) has order \( d/2 \): \( (a^2)^{d/2} = a^{d} \equiv 1 \pmod{p} \).

but if \( f < d/2 \), \( b^f = a^{2f} \not\equiv 1 \pmod{p} \).

What about \( a^4 \) or \( a^6 \)?

If \( 4|d \), \( \text{ord}_p(a^4) = d/4 \) what if \( 2|d \), but \( d/2 \)?

The \( a^2 \) has order \( d/2 \), odd, \( a \) is invertible mod \( d/2 \).

Let \( \overline{a} \) be an inverse, then \( a^2 = (a^2)^{d/2} \). But \( a^2 = (a^2)^{2 \cdot d/2} = (a^2)^{d/2} \equiv a^2 \).

If \( a \), \( b \) are powers of each other, have same order.

If \( b \) power of \( a \) then \( \text{ord}_p(b) \mid \text{ord}_p(a) \).

If reverse also true then \( \text{ord}_p(b) = \text{ord}_p(a) \).

\( \Rightarrow \) if \( 2|d \), \( 4|d \), \( \text{ord}_p(a^4) = d/2 \)

\( \Rightarrow \) if \( 2|d \), \( 6|d \), \( \text{ord}_p(a^6) = d/6 \)

\( \Rightarrow \) if \( 2|d \), \( 3|d \), \( \text{ord}_p(a^6) = \text{ord}(a^2) = d/2 \) since \( 3 \) invertible mod \( d/2 \).

See: if \( j \) is invertible mod \( \text{ord}_m(a) \) then \( a^j \equiv \text{ord}_m(a) = \text{ord}_m(a)^{\phi(d) \cdot j} \).

(If: if \( j \) is an inverse, \( a = (a^j)^{\phi(d)} \).

\( \Rightarrow \) at least \( \phi(d) \) powers of \( a \) of order \( d \).

In general, \( \text{ord}_m(a^i) = \frac{\text{ord}_m(a)}{\gcd(\text{ord}_m(a), i)} \).
Proof of claim: \( d = \text{ord}_m(a), \ e = \gcd(j, d) \)

\[ a^e \text{ has order } \frac{d}{e} \text{ mod } m \]

and \( a^j \) is invertible mod \( \frac{d}{e} \) \( (\gcd(j, \frac{d}{e}) = 1) \)

so \( \text{ord}_m((a^e)^j) = \text{ord}_m(a^e) = \frac{d}{e} \)

so \( \text{ord}_m(a^j) = d = \text{ord}_m(a) \) iff \( j \) invertible prime to \( d \)

Rightarrow \( \phi(d) \) classes of order \( d \)

Recap: \( p \) prime, \( n = p-1 \), \( d | p-1 \), \( a \mod p \) has order \( d \)

\Rightarrow exactly \( \phi(d) \) classes of order \( d \)

If no \( \phi(d) \) element has order \( d \) then have 0 such classes

Endgame: let \( f(d) = \# \text{ classes of order } d \)

Fermat: every class has order \( |n = p-1| \)

so \( \sum_{d | n} f(d) = n = p-1 \)

and \( \sum_{d | n} \phi(d) = n \)

Each summand on top is either equal to summand on bottom or zero. But sums are equal, so no zeroes:

\( f(d) = \phi(d) \) for all \( d \), \( \phi \) in particular

\( f(p-1) = \phi(p-1) \geq 1 > 0 \).